

REMARKS

SPECIFICATION

In the specification, paragraph [0020] has been amended to provide a typographical correction. Paragraph [0022] has been amended to include the descriptive label for element 112 from FIG. 1, namely "Application programs" 112. These amendments to the specification are fully supported by the application as filed, and no new matter is added.

STATUS OF CLAIMS

Claims 8-26 have been cancelled.

No claims have been amended, added, or withdrawn.

Claims 1-7 are currently pending in the application.

SUMMARY OF THE REJECTIONS

Claims 1-3, 7-8, 10-19, and 21 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent Application Publication Number 2003/0048468 A1 of Boldon et al. ("*Boldon* ") in view of U.S. Patent Number 5,937,150 issued to Phan ("*Phan* "). Claims 4-6 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Boldon* in view of *Phan* and in further view of U.S. Patent Application Publication Number 2004/0025042 A1 of Kouznetsov et al. ("*Kouznetsov* "). Claims 9, 20, and 22-26 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Boldon* in view of *Phan* and in further view of U.S. Patent Number 5,956,481 issued to Walsh et al. ("*Walsh* "). The rejections are respectfully traversed.

PRELIMINARY ADMINISTRATIVE MATTER – BASIS OF REJECTIONS

As a preliminary administrative matter, the Applicant notes that the summary of rejections above is based upon the detailed rejections of each claim. Thus, contrary to the introduction of the claim rejections on page 2 of the Final Office Action (which states that all of Claims 1-26 are rejected based on *Boldon* in view of *Phan*), not all of Claims 1-26 have been rejected under 103(a) based on *Boldon* in view of *Phan*. Instead, the basis of the claim rejections are as given above, based upon how each claim is addressed in the Final Office Action.

ARGUMENTS IN REPOSE TO THE REJECTIONS

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

Claim 1 features, in relevant part, at least the following:

“A multi-function peripheral device comprising:

.....[*features omitted for purposes of the following explanation only*]

a **virus protection process** executing in the memory and being configured to perform the steps of:

detecting that a ***request*** for data **to be analyzed for viral infection** has been ***received by*** the multi-function peripheral device over the network **from a network device**; and

in **response to detecting receipt of the request**, *causing the data to be provided from* the multi-function peripheral device to the network device over the network **to enable the data to be analyzed for viral infection at the network device.**” (Emphasis added.)

Thus, Claim 1 features not merely “detecting a ***request*** for data... has been ***received...*** **from a network device**,” but rather that the requested data is “**to be analyzed for viral infection.**” Furthermore, the “**response**” to the request is not merely “*causing the data to be provided...*,” but rather that the data is being provided “**to enable the data to be analyzed for viral infection at the network device.**”

As a result, in the approach of Claim 1 the multi-function peripheral device ***itself*** is **not** detecting whether the data has a viral infection, but rather that another device, namely “**a network device**,” is performing the viral detection of the data that is **provided from** the multi-function peripheral device **to** the network device. In a sense, this approach may be viewed as a form of remote detection of viral infection because one device (e.g., the “network device”) is analyzing data from another device (e.g., the multi-function peripheral device) to see if the data contains a viral infection.

And in the approach of Claim 1, this remote detection is initiated by the network device in the form of “a ***request*** for data **to be analyzed for viral infection**” with the multi-

function peripheral device responding by sending the requested data so that the data can “***be analyzed for viral infection at the network device.***”

In particular, the Applicant notes that Claim 1 is supported in the Application by the embodiment described in Section VII. REMOTE VIRUS PROTECTION in paragraphs [0039-0045] and as illustrated in FIG. 4 and FIG. 5. Specifically, in step 502, MFP 402 receives a request from network device 404 for data to be tested for a viral infection, and in step 504, MFP 402 responds to the request by sending the requested data to network device 404 via network 406. Then in step 506, network device 404 performs virus testing on the data provided by MFP 402, such as by using virus protection tool 412. In step 508, network device 404 provides instructions to MFP 402 when the results of the virus testing show that the data is infected, such as network device 404 instructing MFP 402 to replace the data that was sent, quarantine the infected data, or to delete the infected data. Then in step 510, MFP 402 performs the actions based on the instructions from network device 404 and provides notifications, if appropriate.

(2) INTRODUCTORY DISCUSSION OF *BOLDON*

In contrast, *Boldon* discloses an approach for “virus filtering for **use in peripherals**, such as...printers, scanners, or facsimile machines.” (Abstract; emphasis added.) Specifically, information is **sent to a printer** where the information sent to the printer is scanned for viruses “**by the printer**” to determine whether or not the information contains a virus. (FIGURE; paragraph [0019]; emphasis added; *note* - there is only one FIGURE in *Boldon*, hence there is no figure number and *Boldon* simply refers to the only drawing as the FIGURE.)

Thus, *Boldon*’s approach is intended to provide for scanning of external data coming into a peripheral device, such as a printer, scanner, facsimile machine or the like...” so that a virus that has infected a computing device does not spread to the peripheral device. (Paragraphs [0003-0005].)

(3) THE FINAL OFFICE ACTION’S CITATIONS FROM *BOLDON*

The Final Office Action states that *Boldon* discloses “a peripheral device for detecting a request for data to be analyzed for virus has been received over the network by a network

device (para. 0019, lines 1-7).” However, this statement in the Final Office Action misstates the features of Claim 1 because the request is not received **by** a network device; rather the request is received **by** the multi-function peripheral device **from** the network device.

Furthermore, the cited portion of *Boldon* says nothing about “detecting that a **request** for data **to be analyzed for viral infection** has been **received**...,” little less that such a request has been received “by the multi-function peripheral device ... **from a network device**,” as featured in Claim 1. Rather, *Boldon*’s paragraph [0019] merely restates the content of the FIGURE, which is for an approach for detecting viruses in print jobs at the printing device. While this description and the FIGURE is understood as involving print jobs sent to the printer from another device over a network, there is nothing in *Boldon* to suggest that there is a **request for data to be analyzed for viral infection**.

Instead, this portion of *Boldon* would be understood as disclosing that print jobs are sent to the printer, and before printing, the printer scans the print jobs to see if there are any viruses in the print jobs. At most, the performing of such virus scanning of print jobs received by the printer is in response to a request to print the job being sent, but there is nothing in this portion of *Boldon* or elsewhere that the print job includes a request from the device that sent the print job to perform a virus scan of the print job before performing the printing of the job. There is nothing in *Boldon* that suggests that whatever device sends the print jobs to the printer also sends a request to the printer for the printer to scan the print job for viruses.

The Final Office Action also states that *Boldon* discloses “in response to detecting receipt of the request, causing data to be provided from the multi-function peripheral device to the network device over the network to enable the data to be analyzed for viral infection at the network device (0016, lines 5-14; 0023, lines 1-9).” However, a careful reading of the cited portions of *Boldon* again shows that *Boldon* does not disclose anything about “a **request** for data **to be analyzed for viral infection**...,” as featured in Claim 1, little less that in response to detecting such a request, “*causing the data to be provided* from the multi-function peripheral device to the network device over the network **to enable the data to be analyzed for viral infection**,” as also featured in Claim 1.

Specifically, the first cited portion of *Boldon* from paragraph [0016] merely explains that modern peripherals have greatly expanded functionality, including acting as file servers to keep certain files internally and to send them to other devices when requested, receiving data

in the form of programming language to be used to implement new functionality at the peripheral to change the way the device performs its job, and sending data to other devices based on any number of criteria. (Paragraph [0016].) While this paragraph uses the word “requested,” it is in the context of the peripheral sending a file stored at the peripheral when the peripheral is acting as a file server, but such a request is not “a ***request*** for data **to be analyzed for viral infection...**,” little less that in response to such a request, the data is provided by *Boldon*’s printer to a network device “**to enable the data to be analyzed for viral infection at the network device,**” as featured in Claim 1. In fact, the whole goal of *Boldon*’s approach is to scan print jobs that come into a printer, so it is not feasible that *Boldon* could be understood as sending data to another device when the other device requests that data for the purpose of the other device performing a virus scan.

In addition, the second cited portion of *Boldon* from paragraph [0023] merely explains that the printing device, upon detecting a virus in the information to be printed, deletes the information and/or contacts a system administrator, so as to eliminate the virus or at least prevent the spread of the virus to other printing devices and general-purpose devices. (Paragraph [0023].) Again, this portion of *Boldon* says nothing about “a ***request*** for data **to be analyzed for viral infection...**,” little less that in response to such a request, the data is provided “**to enable the data to be analyzed for viral infection at the network device,**” as featured in Claim 1.

Thus, to summarize the Applicant’s understanding of the Final Office Action’s rejections of Claim 1, it appears that the Final Office Action is using the disclosure in *Boldon* of a printer that scans print jobs for virus as disclosing the two steps performed by the virus protection process that is executing in the memory of the multi-function peripheral of Claim 1. However, in neither the cited portions of *Boldon* or elsewhere does the Applicant see anything about “detecting that a ***request*** for data **to be analyzed for viral infection** has been ***received*** by the multi-function peripheral device over the network **from a network device**” or that in response to such a request, that the data is being provided “**to enable the data to be analyzed for viral infection at the network device.**”

While *Boldon*’s description involves at least a printer and another device sending print jobs to the printer, there is nothing disclosed in *Boldon* about the printer sending a request to the other device for the print job so that the printer can scan the print job for a virus, nor is

there anything in *Boldon* that the other device has requested data from *Boldon* to be scanned for viruses by that other device and that the printer sends the data to that other device in response to such a request. Therefore, to the extent that the Final Office Action is based on the printer in *Boldon* being the “network device” of Claim 1, there is nothing in *Boldon* about the printer requesting the print job from another device for the purpose of performing a virus check on the print job. Rather, *Boldon* is most reasonably understood to describe that the other device sends a print job to the printer in *Boldon*, and at most, sending of that print job would be understood as a request by the other device to the printer to print the print job, but not a request by the other device for the printer to scan the print job for viruses.

As a result, the Applicant respectfully submits that *Boldon* is best understood as disclosing an approach for having a printer scan incoming print jobs for virus, that such print jobs are initiated by other devices instead of *Boldon*’s printer, and that *Boldon*’s printer scans the incoming print jobs for viruses as a precaution against the printer becoming infected with a virus contained in the print job. However, in contrast to *Boldon*’s approach, the approach of Claim 1 is for a multi-function peripheral device that includes a virus protection process configured to perform the steps of “detecting that a ***request*** for data **to be analyzed for viral infection** has been ***received*** by the multi-function peripheral device over the network **from a network device**” and that “in response to detecting receipt of the request, causing the data to be provided from the multi-function peripheral device to the network device over the network **to enable the data to be analyzed for viral infection at the network device.**”

(4) DISCUSSION OF *PHAN*, *KOUZNETSOV*, AND *WALSH*

The Final Office Action relies upon *Phan* as allegedly disclosing a multi-function peripheral device that comprises “a network interface...a graphical user interface...a memory...a scan process...a print process...,” and thus the Final Office Action does not rely upon *Phan* as disclosing any of the features of Claim 1 that the Final Office Action relies upon as being disclosed in *Boldon*. Nevertheless, the Applicant has reviewed *Phan* and yet found nothing in *Phan* related to the features of Claim 1 discussed above.

In addition, while the Final Office Action does not rely upon either *Kouznetsov* or *Walsh* in the rejection of Claim 1, and instead uses those two references in the rejections of

other claims, the Applicant can similarly find nothing in either of *Kouznetsov* or *Walsh* related to the features of Claim 1 discussed above.

(5) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *BOLDON, PHAN, KOUZNETSOV, AND WALSH*

Because *Boldon, Phan, Kouznetsov, and Walsh*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious “detecting a ***request*** for data **to be analyzed for viral infection** has been ***received... from a network device***” and “in **response to detecting receipt of the request**, *causing the data to be provided* from the multi-function peripheral device to the network device...**to enable the data to be analyzed for viral infection at the network device**,” the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

C. CLAIMS 2-7

Claims 2-7 are dependent upon Claim 1, and thus include each and every feature of the corresponding independent claim. Therefore, it is respectfully submitted that Claims 2-6 and are allowable for the reasons given above with respect to Claim 1.

(a) Claim 4

Regarding Claim 4, the Final Office Action states that *Kouznetsov* discloses “receiving replacement data for the multi-function peripheral (paragraph 0161, lines 1-2; paragraph 016, lines 1-2).” As a preliminary matter, it appears that the second reference is incomplete and perhaps refers to one of paragraphs 0162 through 0169, although for the reasons stated herein, the Applicant can find nothing about the relevant features of Claim 4 in any of those paragraphs.

As another preliminary administrative matter, Claim 4 includes additional features that are not even addressed in the rejection of Claim 4 in the Final Office Action. Specifically, Claim 4 does not only feature “receiving replacement data for the multi-function peripheral, but Claim 4 also features “receive replacement data from the network device that has been disinfected” and “replace the data on the multi-function peripheral device with the replacement data.” Thus, it appears to the Applicant that the rejection of Claim 4 based on

Kouznetsov is incomplete because (a) the second citation's paragraph number is missing the final digit and (b) several additional features of Claim 4 are not addressed in the rejection.

Nevertheless, the Applicant respectfully submits that *Kouznetsov* fails to disclose the features of Claim 4, for at least the reasons given herein. First, the cited portion from paragraph [0161] states in its entirety: "A clean record contains a function for removing the malware and repairing files, if possible." While this disclosure may be interpreted as describing the disinfecting of a file that is infected with "malware," there is nothing in this disclosure or elsewhere in *Kouznetsov* that the Applicant has found about a multi-function peripheral device that can "receive replacement data from the network device that has been disinfecting." The Applicant notes that this network device being referred to therein in Claim 4 is the same network device as in Claim 1 (from which Claim 4 depends), and that in Claim 1, that network device both (a) "sent the request [to the multi-function peripheral device] for data to be analyzed for viral infection" and then (b) after the data is "provided from the multi-function peripheral device to the network device," thereby enable[s] the data to be analyzed for viral infection at the network device."

Second, any of the remainder of paragraphs [0162] through [0169] that may have been intended to be referred to in the Final Office Action by the incomplete citation also fail to disclose these features of Claim 4. Paragraph [0162] describes multiple detected malware may use the same clean functions, paragraph [0163] introduces free records, paragraph [0164] describes that deleted records are merged with other free records or added to the free record list, paragraph [0165] describes that replacing a record is the same as deleting the original and adding a new record in its place, paragraph [0166] describes that free records may be set to zero, paragraph [0167] introduces the activity logging module, paragraph [0168] describes that the activity logging subsystem records events for back-end analysis, and paragraph [0169] introduces the logged events of Table 17.

It appears to the Applicant that the Final Office Action may have intended to cite to paragraph [0165], since that paragraph includes the word "replacing" that is similar to the term "replace" used in Claim 4. But again, that explanation by *Kouznetsov* that replacing a record is the same as deleting a record and adding a new record is not the same as replacement data that has been disinfecting, as in Claim 4, little less that such replacement data is received by the multi-function peripheral device from the network device or that the multi-function

peripheral device replaces the data with the replacement data. In fact, paragraph [0165] appears to be nothing more than an explanation that a record is replaced by deleting the record and adding a new record in place of the deleted record, whereas in Claim 4, the replacement data is disinfected by the network device, not merely deleted.

In summary, because *Boldon, Phan, Kouznetsov, and Walsh*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious “receive replacement data from the network device that has been disinfected” and “replace the data on the multi-function peripheral device with the replacement data,” the Applicant respectfully submits that, for at least the reasons stated above, Claim 4 is allowable over the art of record and is in condition for allowance.

(B) Claim 7

Regarding Claim 7, the Final Office Action states that *Boldon* discloses “receive a request from the network device for the multi-function peripheral to quarantine or delete at least a portion of the data that was sent from the multi-function peripheral device to the network device (paragraph 0023, lines 1-5).” However, as discussed above, paragraph [0023] of *Boldon* merely explains that the printing device, upon detecting a virus in the information to be printed, deletes the information and/or contacts a system administrator, so as to eliminate the virus or at least prevent the spread of the virus to other printing devices and general-purpose devices. (Paragraph [0023].) While this portion of *Boldon* does describe the deletion of information that is detected as having a virus, the features of Claim 7 being rejected based upon this portion of *Boldon* do not merely include “delete at least a portion of the data that was sent...”

Instead, the relevant features of Claim 7 are that the multi-function peripheral device is configured to perform the step of “**receive a request** from a network device...” and that that request is for the “multi-function peripheral device to quarantine or delete a portion of the data...” Recall that in Claim 1, from which Claim 7 depends, the analysis of the data for viral infection is not performed by the multi-function peripheral device, but rather the analysis for viral infection is performed at the network device that requests the data being analyzed to be provided to the network device by the multi-function peripheral device. Thus, in Claim 7, it is the network device that requests that the multi-function peripheral device quarantine or delete

the portion of the data that was sent via the steps of Claim 1. This is consistent with Claim 1 being an approach for the network device to detect a viral infection in data requested from the multi-function peripheral device, and thus the network device requests that the multi-function peripheral device act to deal with the viral infection by either quarantining or deleting at least a portion of the data that has the viral infection.

Also regarding Claim 7, the Final Office Action states that *Boldon* discloses “[in] response to receiving the request from the network device to quarantine or delete at least a portion of the data that was sent to the network device, quarantine or delete the at least a portion of the data that was sent from the multi-function peripheral device to the network device (paragraph 0006, lines 4-7; paragraph 0007, lines 4-7; paragraph 0016, lines 5-14.” However, these cited portions of *Boldon* again do not disclose anything about a multi-function peripheral receiving “**a request** from a network device....” and that such a request is for the “multi-function peripheral device to quarantine or delete a portion of the data...,” as featured in Claim 7.

Specifically, the latter portion of paragraph [0006] of *Boldon* describes forwarding information to a printing device that scans the information to see if the information contains a virus, and printing the information if no virus is detected. But this says nothing about a multi-function peripheral receiving “**a request** from a network device....” and that that request is that the “multi-function peripheral device to quarantine or delete a portion of the data...,” as featured in Claim 7.

Also, the latter portion of paragraph [0007] of *Boldon* describes that *Boldon*’s approach includes deleting the information if it contains a virus and/or contacting a system administrator if a virus is found. But again, this says nothing about a multi-function peripheral receiving “**a request** from a network device....” and that that request is that the “multi-function peripheral device to quarantine or delete a portion of the data...,” as featured in Claim 7.

Finally, the latter portion of paragraph [0016] of *Boldon* describes, as discussed above, that modern peripherals have greatly expanded functionality, including acting as file servers to keep certain files internally and to send them to other devices when requested, receiving data in the form of programming language to be used to implement new functionality at the peripheral to change the way the device performs its job, and sending data to other devices

based on any number of criteria. (Paragraph [0016].) While this paragraph uses the word “requested,” it is in the context of the peripheral sending a file stored at the peripheral when the peripheral is acting as a file server, but such a request is not “**a request** from a network device....” and that that request is that the “multi-function peripheral device to quarantine or delete a portion of the data....,” as featured in Claim 7.

In fact, the purpose of Boldon’s approach is for the printer to scan print jobs for viruses and for the printer to then deal with any that are found, and therefore, there is no reason for *Boldon*’s approach to include that some other device besides the printer would request that the printer quarantine or delete the information that the printer detects as having a virus. Rather, *Boldon* merely discloses that the printer scans a print job, and if a virus is found, deletes the print job and/or contacts a system administrator, and there is nothing in these cited portions of *Boldon* or elsewhere about *Boldon*’s printer acting upon a print job in which the printer has detected a virus based upon a request from another device to take such a particular action that is specified by the other device to Boldon’s *printer*.

In summary, because *Boldon*, *Phan*, *Kouznetsov*, and *Walsh*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious “receive a request from the network device for the multi-function peripheral to quarantine or delete at least a portion of the data that was sent from the multi-function peripheral device to the network device” and “in response to receiving the request from the network device to quarantine or delete at least a portion of the data that was sent to the network device, quarantine or delete the at least a portion of the data that was sent from the multi-function peripheral device to the network device,” the Applicant respectfully submits that, for at least the reasons stated above, Claim 7 is allowable over the art of record and is in condition for allowance.

CONCLUSION

The Applicant believes that all issues raised in the Final Office Action have been addressed and that allowance of the pending claims is appropriate. Entry of the amendments and further examination on the merits are respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

/CraigGHolmes#44770/

Craig G. Holmes

Reg. No. 44,770

Date: September 6, 2007

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076